DETAILED ACTION

1. This Office Action is in response to the most recent papers filed on 2/17/2009.

2. Claims 1-5, 8-17 & 19-32 are allowed with examiner's amendment.

Response to Arguments and Amendment

3. Applicant's arguments made in interview conducted January 26, 2009, (those arguments appear below completing the prosecution history) have been fully considered in view of the amended claims and are persuasive. The rejection of claims 1-5, 8-17 & 19-32 have been withdrawn.

Interview Summary

4. The words "and executed" are being added to the amended claim language in the independent claims as shown in the following examiner's amendment to make clear the invention's being tied to a machine.

5. The arguments made by applicant's representative in the previous interview conducted on January 26, 2009 appear immediately below completing the prosecution history.

6. In discussing the amendments to claim 1 applicant's representative's arguments were as follows arguing that the amended claim 1 is not taught:

"Rather, the main cited reference Pantuso teaches establishing network communications with a plurality of computers with firewalls over a network. Once the network communications are established, the information relating to intrusion activity is collected from the firewalls of the I computers utilizing the network. See column 1, lines 57-67. Further, the aforementioned information is transmitted from the firewall associated with the computer to a central server utilizing the network. See column 2, lines 12-15. The information is analyzed and rules are generated based on the information. The rules may then be transmitted to the firewalls of the computers utilizing the network. See column 4, lines 47-67. Claim I, however, teaches communicating the information [related to intrusion activity] from a first security engine to a second security engine via an event manager all being within a single host computer. Pantuso teaches communicating the information obtained from firewalls across a network and not within a computer, as taught by Applicant's invention of claim I. The remaining cited art does not overcome the deficiencies of Dunning. It is further believed the above analysis applies to independent claims 14, 22, and 28 as well."

7. In discussing the amendments to claim 10 applicant's representative's arguments were as follows arguing that the amended claim 10 is not taught:

"Rather, the main cited reference Pantuso teaches establishing network communications with a plurality of computers with firewalls over a network. Once the network communications are established, the information relating to intrusion activity is

collected from the firewalls of the computer utilizing the network. See column I, lines 57-67. Further, the aforementioned information is transmitted from the firewall associated with the computer to a central server utilizing the network. See column 2, lines 12-15. The information is analyzed and rules are generated based on the information. The rules may then be transmitted to the firewalls of the computers utilizing the network. See column 4, lines 47-67. The Applicant's invention of claim 10, however, teaches sending the updated security policy [the rules in Pantuso] to security engines that previously requested the security policy [the rules in Panuso]. Pantuso merely transmits the rules to all computers utilizing the network and does not filter which computers receive the rules. The remaining cited art does not overcome the deficiencies of Dunning."

EXAMINER'S AMENDMENT

8. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

9. Authorization for this examiner's amendment was given in a telephone interview with Michael D. Carter on March 16, 2009.

10. Applicants Claims are amended as follows with the additional claim language added to applicants claims as submitted 2/17/2009 underlined:

1. (Currently Amended) A method comprising:

receiving an event from a first security engine;

identifying a second security engine configured to utilize information contained in the event, wherein the second security engine is unaware of the first security engine; and

communicating the information contained in the event to the second security engine via an event manager, wherein the event corresponds to identifying a password that does not comply with predetermined criteria; and

with the first security engine, the second security engine, and the event manager being included and executed in a single host computer.

2. (Previously Presented) A method as recited in claim 1 wherein the event identifies a password that does not comply with a length criteria.

3. (Previously Presented) A method as recited in claim 1 wherein the event identifies an action performed by the first security engine in response to a detected vulnerability.

4. (Original) A method as recited in claim 1 wherein the first security engine and the second security engine are application programs.

5. (Previously Presented) A method as recited in claim 1 wherein the event identifies a password that does not include one or more required characters.

6-7. (Cancelled).

8. (Original) A method as recited in claim 1 wherein the first security engine is a vulnerability analysis application program.

9. (Original) A method as recited in claim 1 further comprising:

identifying a third security engine configured to utilize information contained in the event; and

communicating the information contained in the event to the third security engine.

10. (Currently Amended) A method as recited in claim 1 further comprising:

receiving an updated security policy;

identifying at least one security engine that previously requested the security policy; and

providing the updated security policy to the identified security engine.

11. (Original) A method as recited in claim 1 further comprising:

receiving a request for data from the first security engine; and

communicating the requested data to the first security engine.

12. (Original) A method as recited in claim 1 further comprising storing information contained in the event in a central location accessible to a plurality of security engines.

13. (Original) One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 1.

14. (Currently Amended) A method comprising:

receiving a security-related event from a first security-related application program, the security-related event being associated with a system state;

identifying information contained in the security-related event;

identifying a second security-related application program associated with the information contained in the security-related event, wherein the second security-related application program is unaware of the first security-related application program;

communicating the information contained in the security-related event to the second security-related application program via an event manager; and

with the first security-related application program, the second security-related application program, and the event manager being included and executed in a single host computer.

15. (Previously Presented) A method as recited in claim 14 wherein the information includes whether a network connection is wired or wireless.

16. (Previously Presented) A method as recited in claim 14 wherein the information includes whether a host computer is accessing a corporate network.

17. (Previously Presented) A method as recited in claim 14 wherein the information includes whether a host computer is accessing an unknown network.

18. (Cancelled).

19. (Original) A method as recited in claim 14 further comprising:

receiving system state information from a third security-related application program; and

storing the system state information such that the system state information is accessible to the first security-related application program and the second security-related application program.

20. (Original) A method as recited in claim 14 further comprising:

identifying a third security-related application program associated with the information contained in the security-related event; and

communicating the information contained in the security-related event to the third security-related application program.

21. (Original) One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 14.

22. (Currently Amended) One or more tangible computer-readable media having stored thereon a computer program executed by one or more processors, comprising:

a first security engine associated with a first type of security attack, the first security engine including configuration to detect a password that does not comply with predetermined criteria;

a second security engine associated with a second type of security attack, wherein the second security engine is unaware of the first security engine;

an event manager coupled to receive events from the first security engine and the second security engine, the event manager further to identify information contained in the events and to identify at least one security engine associated with information contained in a particular event, and further to communicate the information contained in the particular event to the at least one security engine and

with the first security engine, the second security engine, and the event manager being included and executed in a single host computer.

23. (Currently Amended) One or more tangible computer-readable media as recited in claim 22 wherein the information contained in the events identifies a type of security attack.

24. (Currently Amended) One or more tangible computer-readable media as recited in claim 22 wherein the information contained in each event identifies an action taken in response to a security attack.

25. (Currently Amended) One or more tangible computer-readable media as recited in claim 22 wherein the information contained in the events includes system state information.

26. (Currently Amended) One or more tangible computer-readable media as recited in claim 22 further comprising a third security engine coupled to the event manager and associated with a third type of security attack.

27. (Currently Amended) One or more tangible computer-readable media as recited in claim 22 further comprising a storage device coupled to the event manager, the first security engine and the second security engine, the storage device to store event information.

28. (Currently Amended) One or more tangible computer-readable media having stored thereon a computer program that, when executed by one or more processors, causes the one or more processors to:

receive a first security-related event from a first service, the first security-related event corresponding to a network-related aspect of a system state;

identify information contained in the first security-related event;

receive a second security-related event from a second service, wherein the second service is unaware of the first service;

identify information contained in the second security-related event;

communicate information contained in the first security-related event to the second service via an event manager;

communicate information contained in the second security-related event to the first service via the event manager; and

with the first service, the second service, and the event manager being included and executed in a single host computer.

29. (Previously Presented) One or more tangible computer-readable media as recited in claim 28 wherein the first security-related event identifies a particular type of security attack.

30. (Previously Presented) One or more tangible computer-readable media as recited in claim 28 wherein the one or more processors further store the information

contained in the first security-related event and the information contained in the second security-related event for access by other services.

31. (Previously Presented) One or more tangible computer-readable media as recited in claim 28 wherein the one or more processors further communicate information contained in the first security-related event to a third service.

32. (Previously Presented) One or more tangible computer-readable media as recited in claim 28 wherein the first service is associated with a first type of security attack and the second service is associated with a second type of security attack.

Allowable Subject Matter

11. Claims 1-5, 8-17 & 19-32 are allowed. No reason for allowance is needed as the record is clear in light of applicant's arguments and specification.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN A. KAPLAN whose telephone number is (571)-270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434